UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,625	04/28/2006	Audrius Berzanskis	053-03US1	5658

53590 7590 10/25/2007

OPTICUS IP LAW, PLLC
7791 ALISTER MACKENZIE DRIVE
SARASOTA, FL 34240

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
10/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,625	BERZANSKIS ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/28/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 28 April 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter of claim 7. Claim 7 requires a "sifted key," but the specification fails to define the phrase. For the purposes of examination, the Examiner shall construe the phrase to be any data that matches from the random basis performed by the receiver. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,757,912 to Blow, hereinafter Blow, in view of U.S. Patent Application Publication No. 2002/0106084 A1 to Azuma et al., hereinafter Azuma.

7. As per claim 1, Blow teaches a method of performing quantum key distribution (QKD) (column 7, line 57), comprising a random set of bits that can be used to generate a key (column 10, lines 54-67).

8. Blow does not teach encrypting the key bits and using the encrypted key bits to form encrypted qubits.

9. Azuma discloses encrypting information to form encrypted qubits (paragraph 0015, 0054, 0059, 0064, 0072).

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the key bits and use those encrypted key bits to form encrypted qubits, since Azuma states at paragraph 0049 that encrypting the information would prevent an eavesdropper from extracting the original information even if the quantum state was stolen.

11. As per claim 9, Blow teaches a quantum cryptography system, comprising:

a) a quantum key distribution (QKD) that encodes weak optical pulses to form qubits (column 7, lines 57-67).

12. Blow does not teach key bits and basis bits and a classical encryption system operably coupled to the QKD system and adapted to encode at least one of the key bits and the basis bits to form encrypted qubits.

13. Azuma discloses encrypting information to form encrypted qubits (paragraph 0015, 0054, 0059, 0064, 0072).

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the key bits and basis bits and use that encrypted data to form encrypted

qubits, since Azuma states at paragraph 0049 that encrypting the information would prevent an eavesdropper from extracting the original information even if the quantum state was stolen.

15. Claims 2-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blow in view of Azuma as applied to claim 1 above, and further in view of **Applied Cryptography**, to Bruce Schneier, hereinafter Schneier.

16. Regarding claim 2, Blow and Azuma do not teach encrypting the key bits using a stream cipher.

17. Schneier teaches the use of stream ciphers (pages 197-211).

18. One of ordinary skill in the art could have combined a stream cipher in the combined system of Blow and Azuma since Schneier discloses at page 197 that stream ciphers convert plaintext to ciphertext one bit at a time. This would have been the most practical solution since the Applicant is breaking the key into bits, Blow discloses a combination of secret bits used to formulate a key, and Azuma encrypts the data bit by bit to form quantum bits (aka qubits). See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

19. With regards to claim 3, Azuma teaches the use if a password (paragraphs 0044, 0045, 0072, 0076).

20. With regards to claim 4, Azuma teaches decoding the encrypted qubits on the receiving side (paragraph 0067). Schneier discloses the use of stream ciphers (pages 197-211).

21. As per claim 5, Blow teaches a method of performing quantum key distribution (QKD) (column 7, line 57) comprising a first QKD station that generates a random set of bits that can be used to generate a key (column 10, lines 54-67).

22. Schneier teaches generating a key stream using a key stream generator and then XORing that data to the plain text data to produce the stream of ciphertext bits (page 197).

23. One of ordinary skill in the art could have combined generate a pad (aka key stream) and XOR the pad with the key bits since Schneier discloses at page 197 that stream ciphers convert plaintext to ciphertext one bit at a time. This would have been the most practical solution since the Applicant is breaking the key into bits and Blow discloses a combination of secret bits used to formulate a key. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

24. Blow and Schneier do not teach modulating weak optical pulses using the encrypted key bits to generate encrypted qubits.

25. The Applicant admits in the "Background Art" section of the specification that quantum key distribution involves establishing a key between a sender and receiver utilizing weak optical signals (page 2, Amendment to the Specification, 4/28/06). Since all of the references deal with quantum communications they all involved weak optical signals.

26. Azuma discloses encrypting information to form encrypted qubits (paragraph 0015, 0054, 0059, 0064, 0072).

27. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modulate weak optical pulses using the encrypted key bits to generate encrypted qubits, since Azuma states at paragraph 0049 that encrypting the information would prevent an eavesdropper from extracting the original information even if the quantum state was stolen.

28. Regarding claim 6, Azuma discloses "Quantum Cryptography: Public Key Distribution and Coin Tossing" to C.H. Bennett et al., hereinafter Bennett, at paragraph 0002. Bennett discloses that Bob (the receiver) decides randomly for each photon received whether to measure the photon rectilinear polarization or diagonal polarization (see Section III, page 3, first paragraph).

29. Azuma teaches decoding the encrypted qubits on the receiving side (paragraph 0067). Schneier discloses the use of stream ciphers, specifically XORs to encrypt/decrypt a stream (pages 197-211).

30. With regards to claim 7, Azuma teaches establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station (paragraph 0007, i.e. results obtained from the observation bases on the Alice and Bob sides that match are adopted as data).

31. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend, hereinafter Townsend, in view of U.s. Patent Application Publication No. 2006/0120529 A1 to Gisin et al., hereinafter Gisin, and further in view of Schneier in view of Azuma.

32. As per claim 8, Townsend teaches a QKD system, comprising:

a) a first QKD station (Figure 4 [block 1]) having:

a. an optical radiation source adapted to emit weak optical pulses of radiation (Figure 4 [block 48], column 4, lines 34-48, column 6, lines 41-63);

d. a modulator arranged to receive the weak optical pulses and adapted to modulate the polarization or phase of the weak optical pulses based on the encrypted key bits to form encrypted qubits (Figure 4 [block 49], column 4, lines 34-55);

b) a second QKD station (Figure 4 [block 2]) optically coupled to the first QKD station (Figure 4 [block 3]) and having:

a. a second modulator adapted to receive and randomly polarization-modulate or phase-modulate the encrypted qubits (Figure 4 [block 52], column 4, lines 34-55, column 6, lines 41-63);

b. a detector for detecting the modulated encrypted qubits (Figure 2 [block 10], column 6, lines 1-40).

33. Townsend does not teach a first random number generator adapted to generate random numbers for use as first key bits.

34. Gisin teaches the use of a random number generator to prepare random quantum states (Figure 1 [blocks 14, 44], paragraph 0026, claim 7).

35. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a random number generator to generate random numbers for the key bits, since Schneier states at page 197 that a randomized key stream allows for perfect security since patterns and strings of similar numbers can result in the key being determined by an eavesdropper.

36. Townsend and Gisin do not teach a first e/d module coupled to the first random number generator to encrypt the key bits thereby forming encrypted key bits and a second e/d module coupled to the detector and adapted to recover from the modulated encrypted qubits second key bits corresponding to the first key bits.

37. Azuma discloses encrypting information to form encrypted qubits (paragraph 0015, 0054, 0059, 0064, 0072) and decoding the encrypted qubits on the receiving side (paragraph 0067).

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to an encryption and decryption module on both the transmitting and receiving side, since Azuma states at paragraph 0049 that encrypting the information would prevent an eavesdropper from extracting the original information even if the quantum state was stolen.

Conclusion

39. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

40. The following patents are cited to further show the state of the art with respect to quantum cryptography, such as:

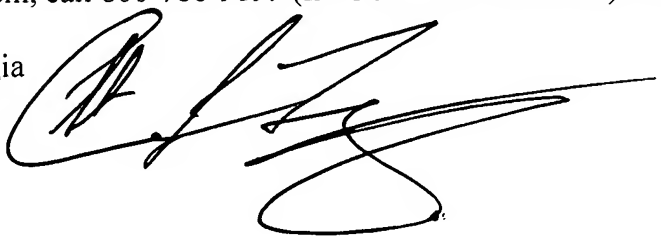
United States Patent No. 7,035,411 B2 to Azuma et al., which is cited to show the patent that issued from the application used to reject the claims of the instant application.

41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

42. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

43. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



Clf